

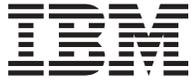


BladeCenter

Management Module User's Guide







@server

BladeCenter

Management Module User's Guide

**Note:** Before using this information and the product it supports, read the general information in “Notices” on page 25.

**First Edition (November 2002)**

**© Copyright International Business Machines Corporation 2002. All rights reserved.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

# Safety

Before installing this product, read the Safety Information.

قبل تركيب هذا المنتج، يجب قراءة الملاحظات الأمنية

Antes de instalar este produto, leia as Informações de Segurança.

在安装本产品之前，请仔细阅读 **Safety Information** (安全信息)。

安裝本產品之前，請先閱讀「安全資訊」。

Prije instalacije ovog produkta obavezno pročitajte Sigurnosne Upute.

Před instalací tohoto produktu si přečtěte příručku bezpečnostních instrukcí.

Læs sikkerhedsforskrifterne, før du installerer dette produkt.

Lees voordat u dit product installeert eerst de veiligheidsvoorschriften.

Ennen kuin asennat tämän tuotteen, lue turvaohjeet kohdasta Safety Information.

Avant d'installer ce produit, lisez les consignes de sécurité.

Vor der Installation dieses Produkts die Sicherheitshinweise lesen.

Πριν εγκαταστήσετε το προϊόν αυτό, διαβάστε τις πληροφορίες ασφάλειας (safety information).

לפני שתתקינו מוצר זה, קראו את הוראות הבטיחות.

A termék telepítése előtt olvassa el a Biztonsági előírásokat!

Prima di installare questo prodotto, leggere le Informazioni sulla Sicurezza.

製品の設置の前に、安全情報をお読みください。

본 제품을 설치하기 전에 안전 정보를 읽으십시오.

Пред да се инсталира овој продукт, прочитајте информацијата за безбедност.

Les sikkerhetsinformasjonen (Safety Information) før du installerer dette produktet.

Przed zainstalowaniem tego produktu, należy zapoznać się z książką "Informacje dotyczące bezpieczeństwa" (Safety Information).

Antes de instalar este produto, leia as Informações sobre Segurança.

Перед установкой продукта прочтите инструкции по технике безопасности.

Pred inštaláciou tohto zariadenia si pečítajte Bezpečnostné predpisy.

Pred namestitvijo tega proizvoda preberite Varnostne informacije.

Antes de instalar este producto, lea la información de seguridad.

Läs säkerhetsinformationen innan du installerar den här produkten.

**Statement 1:**



**DANGER**

**Electrical current from power, telephone, and communication cables is hazardous.**

**To avoid a shock hazard:**

- **Do not connect or disconnect any cables or perform installation, maintenance, or reconfiguration of this product during an electrical storm.**
- **Connect all power cords to a properly wired and grounded electrical outlet.**
- **Connect to properly wired outlets any equipment that will be attached to this product.**
- **When possible, use one hand only to connect or disconnect signal cables.**
- **Never turn on any equipment when there is evidence of fire, water, or structural damage.**
- **Disconnect the attached power cords, telecommunications systems, networks, and modems before you open the device covers, unless instructed otherwise in the installation and configuration procedures.**
- **Connect and disconnect cables as described in the following table when installing, moving, or opening covers on this product or attached devices.**

<b>To Connect:</b>	<b>To Disconnect:</b>
1. Turn everything OFF.	1. Turn everything OFF.
2. First, attach all cables to devices.	2. First, remove power cords from outlet.
3. Attach signal cables to connectors.	3. Remove signal cables from connectors.
4. Attach power cords to outlet.	4. Remove all cables from devices.
5. Turn device ON.	

**Statement 8:**



**CAUTION:**

Never remove the cover on a power supply or any part that has the following label attached.



Hazardous voltage, current, and energy levels are present inside any component that has this label attached. There are no serviceable parts inside these components. If you suspect a problem with one of these parts, contact a service technician.

**Statement 21:**



**CAUTION:**

Hazardous energy is present when the blade is connected to the power source. Always replace the blade cover before installing the blade.



---

## Introducing the BladeCenter management module

This *Management Module User's Guide* contains information about configuring the management module and managing the IBM® @server BladeCenter™ unit and blade servers.

Your BladeCenter unit comes with one hot-swap management module in the management bay.

The management module functions as a service processor and a keyboard/video/mouse (KVM) multiplexer for the multiple blade servers. You configure the BladeCenter unit and modules through the management module, configuring such information as the switch IP addresses. The management module provides the following external connections: keyboard, mouse, and video for use by a local console, and one RJ-45 connector for a 10/100 Mbps Ethernet remote management connection.

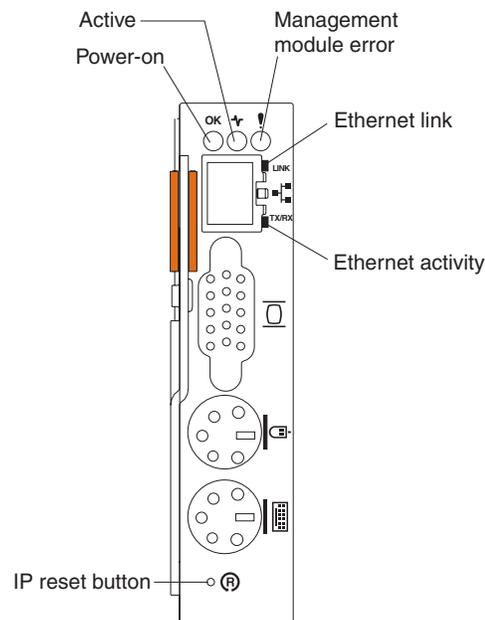
The service processor in the management module communicates with the service processor in each blade server for such functions as:

- Blade server power-on requests
- Blade server error and event reporting
- Blade server requests for keyboard, mouse, and video
- Blade server requests for diskette drive, CD-ROM drive, and USB port

The management module also communicates with the switch modules, power modules, blower modules, and blade servers in the BladeCenter unit to detect their presence or absence and any error conditions, sending alerts when required.

---

## Management module controls and indicators



**Management module LEDs:** These LEDs provide status information about the management module and remote management connection. For additional

information, see the “Light Path Diagnostics” section in the *Hardware Maintenance Manual and Troubleshooting Guide* on the IBM *BladeCenter Documentation CD*.

- **Power-on:** When this green LED is lit, the management module has power.
- **Active:** When this green LED is lit, it indicates that this management module is actively controlling the BladeCenter unit.
- **Management module error:** When this amber LED is lit, it indicates that an error has been detected somewhere on this management module. When this indicator is lit, the system error LED on each of the BladeCenter system LED panels is also lit.
- **Ethernet link:** When this green LED is lit, there is an active connection through the port to the network.
- **Ethernet activity:** When this green LED is flashing, it indicates that there is activity through the port over the network link.

**Management module IP reset button:** Do not press this button unless you intend to erase your configured IP addresses for the management module and lose connection with the remote management station, the switch modules, and the blade servers. If you press this button, you will need to reconfigure the management module settings (see the information beginning with “Setting up the remote connection” on page 5 for instructions).

Press this recessed button to reset the IP configuration of the management module network interfaces (Ethernet 1, Ethernet 2, gateway address, and so forth) to the factory defaults and then restart the management module.

Use a straightened paper clip to press the button.

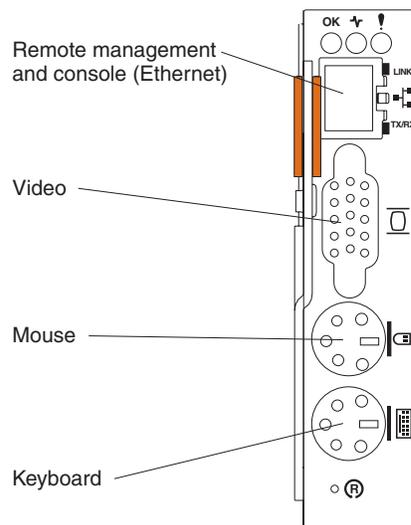
---

## Management module input/output connectors

The management module has the following I/O connectors:

- One video
- One PS/2<sup>®</sup> keyboard
- One PS/2 mouse
- One 10/100 Mbps Ethernet for remote console and management

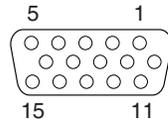
The following illustration shows the I/O connectors on the management module.



## Video connector

Your BladeCenter management module contains one standard video connector. The integrated video controller on each blade server is compatible with SVGA and VGA and communicates through this video port.

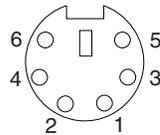
Use this connector to connect a video monitor to the BladeCenter unit.



## Keyboard connector

Your BladeCenter management module contains one PS/2-style keyboard connector.

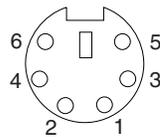
Use this connector to connect a PS/2 keyboard to the BladeCenter unit.



## Mouse connector

Your BladeCenter management module contains one PS/2-style mouse connector.

Use this connector to connect a PS/2 mouse to the BladeCenter unit.



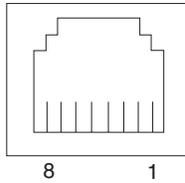
## Remote management and console Ethernet connector

Your BladeCenter management module contains one 10/100 Mb Ethernet connector that provides the remote connection to the network management station on the network.

Use this port for remote management and remote console.

The network management station, through this port, can access control functions running in the service processor on each blade server or within each switch module. However, it cannot use this port to communicate with application programs running in the blade servers. The network management station must direct those communications through a network connected to the external ports in the switch modules in the BladeCenter unit.

The following illustration shows the Ethernet connector that is on the management module.



---

## Configuring the management module and BladeCenter unit

When the BladeCenter unit is started, it automatically configures the remote management port on the management module, so that you can configure and manage the BladeCenter unit and blade servers. You configure and manage the BladeCenter unit remotely, through the management module, using the Web-based user interface.

**Note:** You can also configure the switch modules directly through an external switch module port, using a telnet interface or a Web browser. See the documentation that comes with the switch module for more information.

For the management module to communicate with the blade servers in the BladeCenter unit, you will need to configure the IP addresses for the following internal and external ports:

- Remote management port (out-of-band) on the management module. The initial autoconfiguration enables you to connect to the network management station in order to configure the port completely and to configure the rest of the BladeCenter unit.
- Internal Ethernet port on the management module for communication with the Ethernet switch modules.
- The internal Ethernet management port on each Ethernet switch module, for communication between the management module and the Ethernet switch module. You configure this port by configuring the IP address for the switch module.

To communicate with the blade servers for such functions as deploying an operating system or application program, you also will need to configure at least one external (in-band) port on an Ethernet switch module. See the *IBM @server BladeCenter Type 8677 User's Guide* for information about configuring external ports on Ethernet switch modules.

The management module supports the following Web browsers for remote access. The Web browser that you use must be Java-enabled, must support JavaScript 1.2 or later, and must have the Java 1.4 Plug-In installed.

- Microsoft® Internet Explorer 4.0 (with Service Pack 1), or later
- Netscape Navigator 4.72, or later (version 6.0 is not supported)

**Notes:**

1. For best results when using the Web browser, set the resolution on your monitor to 800 x 600 pixels or higher and 256 colors.
2. The Web interface does not support the double-byte character set (DBCS) languages.

The Web-based user interface communicates with the management and configuration program that is part of the firmware that comes with the management module. You can use this program to perform tasks such as:

- Define the login IDs and passwords
- Select recipients for alert notification of specific events
- Monitor the status of the BladeCenter unit and blade servers
- Control the BladeCenter unit and blade servers
- Access the switch modules to configure them
- Change the drive startup sequence in a blade server
- Set the date and time
- Remote control
- Change ownership of the keyboard, video, and mouse
- Change ownership of the CD-ROM drive, diskette drive, and USB port

**Note:** The IBM Director program is a system-management product that comes with the BladeCenter unit. To configure the remote alert recipients for IBM Director over LAN, the remote alert recipient must be an IBM Director-enabled server.

You also can use the management and configuration program to view some of the blade server configuration settings. See “Using the management and configuration program” on page 7 for more information.

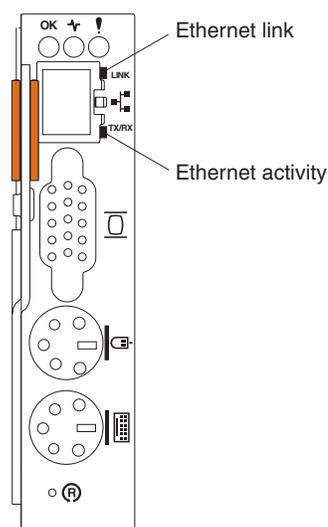
## Setting up the remote connection

To configure and manage the BladeCenter unit and blade servers, you must first set up the remote connection through the Ethernet port on the management module.

### Cabling the Ethernet port

Complete the following steps to connect the Ethernet cable to the management module:

1. Connect one end of a Category 5 or higher Ethernet cable to the Ethernet port on the management module. Connect the other end of the Ethernet cable to the network.
2. Check the Ethernet LEDs to ensure that the network connection is working. The following illustration shows the locations of the Ethernet LEDs.



#### Ethernet link LED

When this green LED is lit, there is an active connection through the port to the network.

### Ethernet activity LED

When this green LED is flashing, it indicates that there is activity through the port over the network link.

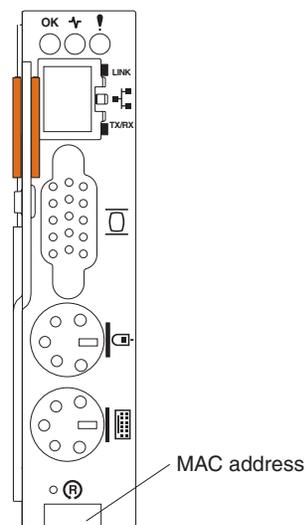
### Configuring the management module for remote access

After you connect the management module to the network, the Ethernet port connection is configured in one of the following ways:

- If you have an accessible, active, and configured dynamic host configuration protocol (DHCP) server on the network, the host name, IP address, gateway address, subnet mask, and DNS server IP address are set automatically.
- If the DHCP server does not respond within two minutes after the port is connected, the management module uses the static IP address and subnet address.

Either of these actions enables the Ethernet connection.

If you do not want to use the default static values, you can configure the static IP address, host name, and subnet mask for the management module through the Web interface. The default IP address is 192.168.70.125, the default subnet address is 255.255.255.0, and the default hostname is MMxxxxxxxxxxx, where xxxxxxxxxxxx is the burned-in medium access control (MAC) address. The MAC address is on a label on the management module, below the IP reset button.



**Important:** Pressing the IP reset button on the management module replaces the configured IP addresses for the management module with the factory default IP addresses, and loses the connection with the remote management station, the switch modules, and the blade servers. If you press this button, you will need to reconfigure the management module settings.

**Note:** If the IP configuration is assigned by the DHCP server, the network administrator can use the MAC address of the management module network interface to find out what IP address and host name are assigned.

### Communicating with the IBM Director software

The IBM Director program is a system-management product that comes with the BladeCenter unit. The IBM Director software communicates with the BladeCenter through the Ethernet port on the management module.

To communicate with the BladeCenter unit, the IBM Director software needs a managed object (in the Group Contents pane of the IBM Director Management Console main window) that represents the BladeCenter unit. If the BladeCenter management module IP address is known, the network administrator can create an IBM Director managed object for the unit. If the IP address is not known, the IBM Director software can automatically discover the BladeCenter unit (out-of-band, using the Ethernet port on the BladeCenter management module) and create a managed object for the unit.

In order for the IBM Director software to discover the BladeCenter unit, your network must initially provide connectivity from the Director server to the BladeCenter management module Ethernet port. To establish connectivity, the management module attempts to use DHCP to acquire its initial IP address for the Ethernet port. If the DHCP request fails, the management module uses a static IP address. Therefore, the DHCP server (if used) must be on the management LAN for your BladeCenter unit.

**Notes:**

1. All management modules are preconfigured with the same static IP address. You can use the management module Web interface to assign a new static IP address for each BladeCenter unit. If DHCP is not used and you do not assign a new static IP address for each BladeCenter unit before attempting to communicate with the IBM Director software, only one BladeCenter unit at a time can be added onto the network for discovery. Adding multiple units to the network without a unique IP address assignment for each BladeCenter unit results in IP address conflicts.
2. For switch communication with the IBM Director server through the management module external Ethernet port, the switch module internal network interface and the management module internal and external interfaces must be on the same subnet.

## Using the management and configuration program

This section provides the instructions for using the management and configuration program in the management module.

### Starting the management and configuration program

Complete the following steps to start the management and configuration program:

1. Open a Web browser. In the address or URL field, type the IP address or host name defined for the management module remote connection (see “Configuring the management module for remote access” on page 6 for more details).

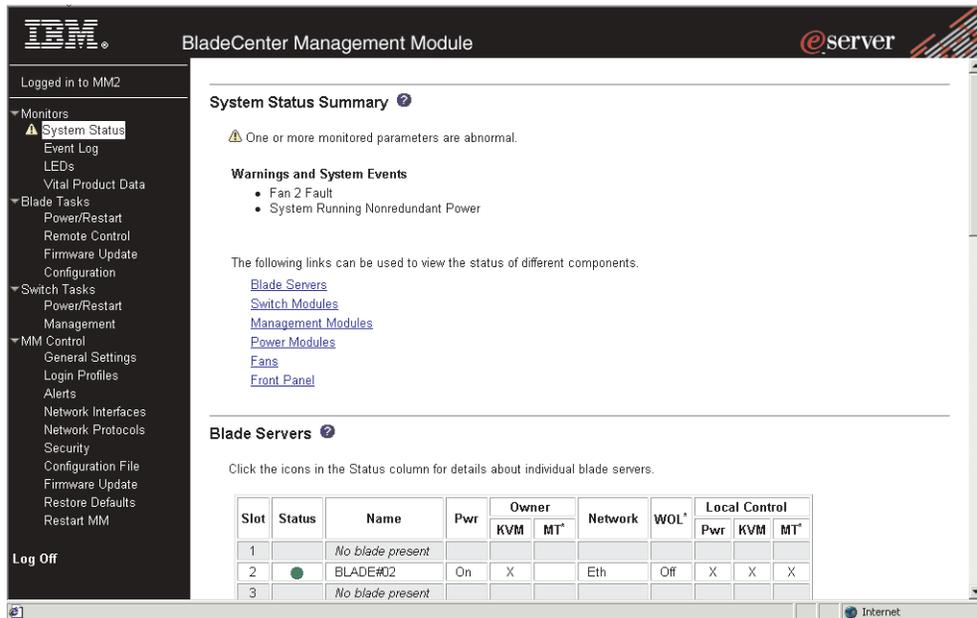
The Enter Network Password window opens.

2. Type your user name and password. If you are logging in to the management module for the first time, you can obtain your user name and password from your system administrator. All login attempts are documented in the event log.

**Note:** The initial user ID and password for the management module are:

- User ID: USERID (all capital letters)
  - Password: PASSW0RD (note the zero, not O, in PASSW0RD)
3. Follow the instructions that appear on the screen. Be sure to set the timeout value you want for your Web session.

The BladeCenter management and configuration window opens.



## Management and configuration program options

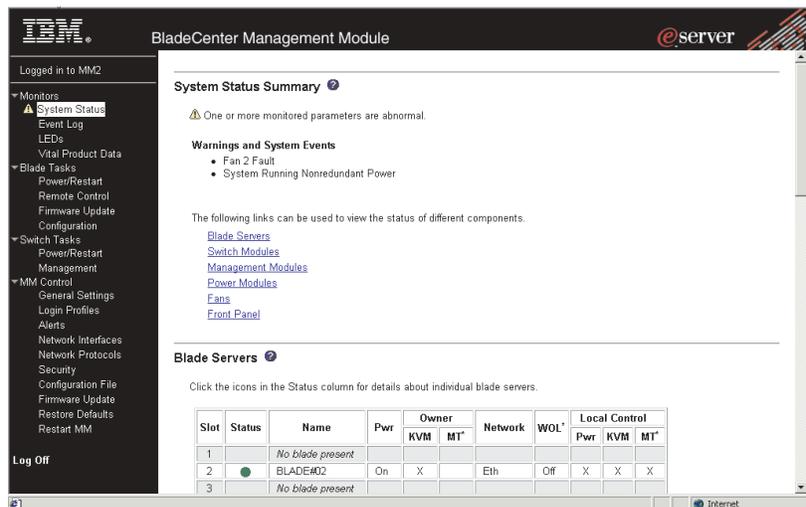
From the management and configuration program main menu, you can select settings that you want to view or change.

The navigation pane (at the left on the management module window) contains navigational links that you use to manage your BladeCenter unit and check the status of the components (modules and blade servers). Descriptions of the links are as follows:

### Monitors

Use the choices in this section to view the status, settings, and other information for components in the BladeCenter unit.

#### System status



Select this choice to view the overall system status, a list of outstanding events that require immediate attention, and the overall status of each of the blade servers and switch modules.

**Blade Servers:**

- **Bay** - The lowest-number bay the blade server occupies.
- **Status** - An icon that indicates good, warning, or bad for the particular blade server. Click the icon for more detailed status information.
- **Name** - The name of the blade server.
- **Pwr** - The power state (on or off) of the blade server.
- **Owner** - An indication of whether the blade server is the current owner of the following BladeCenter resources:
  - **KVM** - Keyboard, video, and mouse.
  - **MT** - The CD-ROM drive, diskette drive, and USB port.
- **Network** - An indication of which network interfaces are on the blade server (Ethernet or Fibre Channel).
- **WOL** - An indication of whether the Wake on LAN<sup>®</sup> feature is currently enabled for the blade server.
- **Local Control** - an indication of whether the following options are enabled:
  - Local power control
  - Local keyboard, video, and mouse switching
  - Local CD-ROM drive, diskette drive, and USB port switching

**Switch modules:**

- **Bay** - The number of the bay the switch module occupies.
- **Status** - Icon that indicates good, warning, or bad for the particular switch module.
- **Type** - The network interface (Ethernet or Fibre Channel) the switch module uses.
- **MAC Address** - The medium access control (MAC) address of the switch module.
- **IP Address** - The IP address of the switch module.
- **Power** - The power state (on or off) of the switch module.
- **Details** - Text information about the status of the switch module.

**Management module:**

- **Bay** - The number of the bay that the management module occupies.
- **Status** - An icon that indicates good, warning, or critical for the particular management module. Click the icon for more detailed status information.
- **IP Address** - The IP address of the remote connection (external Ethernet port) on the management module.

**Power Modules:**

- **Bay** - The number of the bay that the power module occupies.
- **Status** - An icon that indicates good, warning, or critical for the particular power module.
- **Details** - Text information about the status of the power module.

## Blowers:

- **Bay** - The number of the bay that the blower module occupies.
- **Status** - An icon that indicates good, warning, or critical for the particular blower module.
- **Speed** - The current speed of the blower module, as a percentage of the maximum revolutions per minute (RPMs). The blower speed varies with the thermal load. An entry of *Offline* indicates that the blower is not functioning.

**Front panel:** The temperature status for the front of the BladeCenter unit.

## Event log

The screenshot shows the IBM BladeCenter Management Module interface. The left sidebar contains a navigation menu with the following items: System Status (selected), Event Log, LEDs, Hardware VPD, Firmware VPD, Blade Tasks (Power/Restart, Remote Control, Firmware Update, Configuration), Switch Tasks (Power/Restart, Management), MM Control (General Settings, Login Profiles, Alerts, Network Interfaces, Network Protocols, Security, Configuration File, Firmware Update, Restore Defaults, Restart MM), and Log Off.

The main content area is titled "Event Log" and features a filter table:

Severity	Source	Date	Filter
<input type="checkbox"/> Error	BLADE_05	10/16/02	<input type="button" value="Filter"/>
<input type="checkbox"/> Warning	SERVPROC		<input type="button" value="Disable Filter"/>
<input type="checkbox"/> Info			

Below the filter table, a note states: "Note: Hold down Ctrl to select more than one option. Hold down Shift to select a range of options."

The event log table contains the following entries:

Index	Sev	Source	Date/Time	Text
1	I	SERVPROC	10/16/02, 13:24:38	Remote Login Successful. Login ID: "USERID" from WEB browser at IP@=160.0.0.33"
2	E	BLADE_05	10/16/02, 13:18:38	(SN#229X7P J1NN) POSTBIOS: I9900E50 AC power has been restored.
3	E	BLADE_05	10/16/02, 13:18:35	(SN#229X7P J1NN) POSTBIOS: I9900E50 AC power has been restored.
4	I	BLADE_05	10/16/02, 13:17:54	(SN#11NNP229X7P) Blade Server Powered Up
5	I	SERVPROC	10/16/02, 13:17:38	Blade Server 5 was installed.
6	I	SERVPROC	10/16/02, 13:16:31	Blade Server 5 was removed.
7	I	BLADE_05	10/16/02, 13:16:23	(SN#229X7P J1NN) Blade Server Powered Down
8	I	SERVPROC	10/16/02, 12:40:15	System log cleared

At the bottom of the event log area, there are three buttons: "Reload Log", "Clear Log", and "Save Log as Text File".

Select this choice to view entries that are currently stored in the management module event log. This log includes entries for events that are detected by the blade servers. The log displays the most recent entries first. Information about all remote access attempts is recorded in the event log, and the management module sends out the appropriate alerts if configured to do so.

You can sort and filter entries in the event log.

## LEDs

The screenshot shows the BladeCenter Management Module interface. The top bar includes the IBM logo, the text 'BladeCenter Management Module', and the '@server' logo. A navigation menu on the left lists various system management options. The main content area is titled 'LEDs' and is split into two sections:

**Front Panel LEDs**

LED	Status	Action
System error		
Information		Off
Temperature		
Identity		On Off Blink

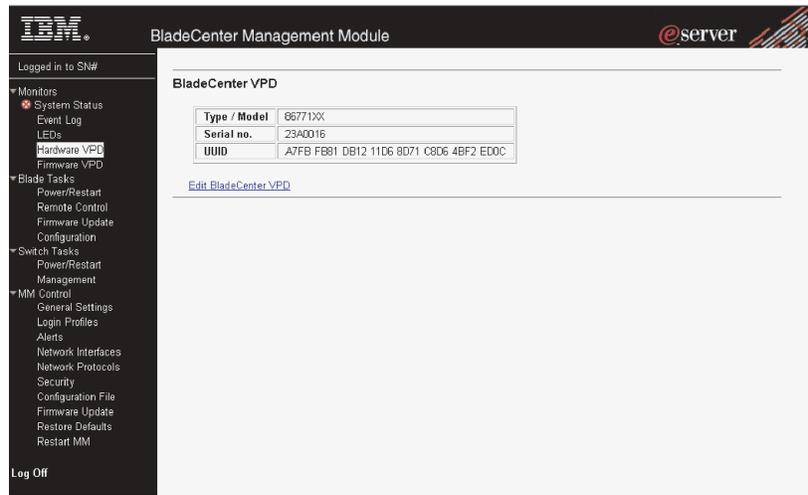
**Blade Server LEDs**

Bay	Name	Error	Information	KVM	MT	Identity
1	SN#229/7P J1NN			Off		
2	No blade present					
3	No blade present					
4	No blade present					
5	No blade present					
6	No blade present					
7	No blade present					
8	No blade present					
9	No blade present					
10	No blade present					
11	No blade present					

Select this choice to view the state of the BladeCenter system LED panel and blade server control panel LEDs. You also can use this choice to turn off the information LED and turn on, turn off, or blink the location LED on the BladeCenter unit and the blade servers.

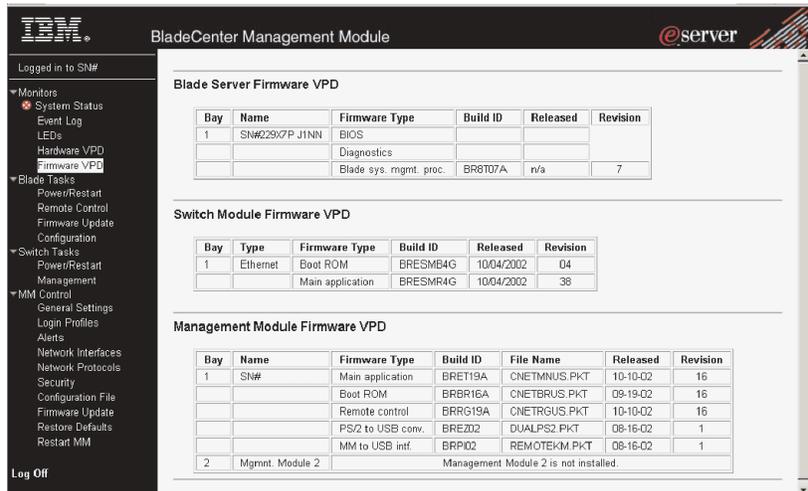
- **Front Panel LEDs** - The state of the following LEDs on the BladeCenter system LED panel. You can change the state of the information and location LEDs.
  - Information
  - System error
  - Over temperature
  - Location
- **Blade Server LEDs** - The state of the following LEDs on the blade server control panel. You can change the state of the information and location LEDs.
  - Power
  - Information
  - Error
  - Location
  - Keyboard, video, and monitor select
  - Media (CD-ROM, diskette drive, USB port) select

## Hardware VPD



Select this choice to view the hardware vital product data (VPD) for the BladeCenter unit. When the BladeCenter unit is started, the management module collects the vital product data and stores it in nonvolatile memory. The management module then modifies the stored VPD as components are added to or removed from the BladeCenter unit. You can access this information at any time from almost any computer.

## Firmware VPD



Select this choice to view the vital product data (VPD) for the firmware in all blade servers and the switch modules and management module in the BladeCenter unit. The firmware VPD identifies the firmware type, build ID, release date, and revision number. The VPD for the firmware in the management module includes the file name of the firmware components.

## Blade tasks

Select the choices in this section to view and change the settings or configurations of blade servers in the BladeCenter unit.

## Power/restart

BladeCenter Management Module

Blade Power / Restart

Select one or more blade servers(s) using the checkboxes in the first column and then click on one of the links below the table to perform the desired action.

<input type="checkbox"/>	Bay	Name	Pwr	Local Pwr Control	Wake on LAN	Console Redirect
<input type="checkbox"/>	1	SN#229/K7P J1NN	On	Enabled	On	
	2	No blade present				
	3	No blade present				
	4	No blade present				
	5	No blade present				
	6	No blade present				
	7	No blade present				
	8	No blade present				
	9	No blade present				
	10	No blade present				
	11	No blade present				
	12	No blade present				
	13	No blade present				
	14	No blade present				

[Power On Blade](#)  
[Power Off Blade](#)  
[Restart Blade](#)

Select this choice to perform the following actions on any blade server in the BladeCenter unit:

- Turn on or turn off the selected blade server (set the power state on or off).
- Enable or disable local power control. When local power control is enabled, a local user can turn on or turn off the blade server by pressing the power-control button on the blade server.
- Enable or disable the Wake on LAN feature.
- Restart the blade server or the service processor in the blade server.

Select the blade servers you want to perform an action on; then, click the appropriate link below the table for the action you want to perform.

## Remote control

BladeCenter Management Module

Remote Control Status

KVM owner: Blade1 - SN#229/K7P J1NN since 10/16/2002 14:12:20  
 Media tray owner: Blade1 - SN#229/K7P J1NN since 10/16/2002 14:12:20  
 Console redirect: No session in progress.

[Refresh](#)

Redirect Server Console

To disable the buttons located on the blade servers for KVM and media tray switching, check the boxes below and click "Save". Click "Redirect Server Console" to start a console redirect session. This session will allow you to access the video console of the KVM owner blade and have full keyboard and mouse control. You can also change KVM and media tray ownership during this session.

Disable local KVM switching  
 Disable local media tray switching

[Save](#) [Redirect Server Console](#)

Select this choice to:

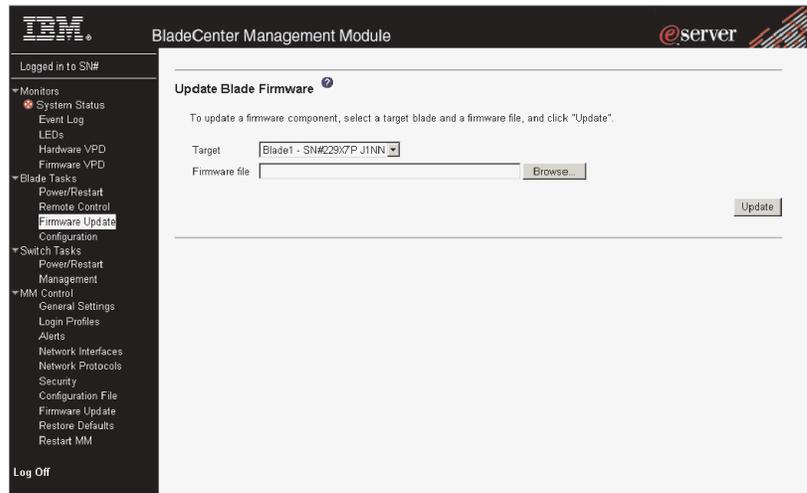
- View the current owners of the keyboard, monitor, and mouse (KVM), and of the CD-ROM drive, diskette drive, and USB port (Media tray).

- View the details of any remote control session currently active (user ID, client IP address, start time).
- Redirect a blade server console to the remote console. On the remote console, you can:
  - Disable local switching of the KVM and of the media tray for all blade servers until explicitly enabled again. This prevents a local user from switching the console display to a different blade server while you are performing tasks.
  - Change the owner of the KVM and of the media tray.
  - View the current blade server display.
  - Control the blade server as if you were at the local console, including restarting the blade server and viewing the POST process, with full keyboard and mouse control.

**Notes:**

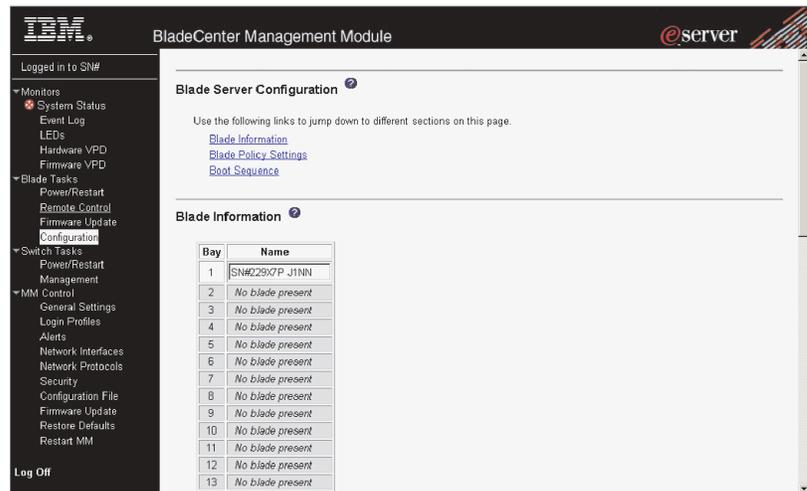
1. Only one remote control session is allowed at a time. If a remote control session is already active, you can end the current session and start a new one.
2. The timeout value for a remote control session is the same as the timeout value that you set for the Web session when you logged in.
3. When you redirect a blade server Linux X Window System session console to the remote console, the ability of the remote console applet to accurately track the location of the mouse cursor depends on the configuration of X-Windows. Complete the following procedure to configure the X Window System for accurate mouse tracking. Type the commands through the remote console or at the keyboard attached to the BladeCenter unit. Note that the changes require root privileges.
  - a. Enter the following commands:
    - `init 3` (Switch to text mode if necessary)
    - `rmmmod mousedev` (Unload the mouse driver module)
  - b. Add the following statement to `.xinitrc` in the user's home directory:
    - `xset m 1 1` (Turn off mouse acceleration)
  - c. Add the following statement to `/etc/modules.conf`:
    - `options mousedev xres=X yres=Y` (Notify the mouse driver of the video resolution) where X and Y specify the video resolution
  - d. Enter the following commands:
    - `insmod mousedev` (Reload the mouse driver module)
    - `init 5` (Return to GUI mode if necessary)

## Firmware update



Select this choice to update the service processor firmware on a blade server. Select the target blade server and the firmware file to use for the update; then, click **Update**. You can obtain the firmware files from the IBM Support Web site at <http://www.ibm.com/pc/support/>.

## Configuration



Select this choice to:

- Define a name for a blade server.
- View or define the startup (boot) sequence for one or more blade servers. The startup sequence prioritizes the following boot-record sources for a blade server:
  - IDE drive 1 (HDD1)
  - IDE drive 2 (HDD2)
  - CD-ROM
  - Diskette
  - Network
  - **PXE** - Attempt a PXE/DHCP network startup the next time the selected blade server is turned on or restarted.

**Note:** In order to use the CD-ROM drive or diskette drive as a boot-record source for a blade server, the blade server must have been designated as the owner of the CD-ROM drive, diskette drive, and USB port. You set ownership either by pressing the CD/diskette/USB select button on the blade server or through the “Remote Control” choice described on page 13.

## Switch Tasks

Select the choices in this section to view and change the settings or configuration on network-interface switch modules in the BladeCenter unit.

### Power/Restart

The screenshot shows the 'BladeCenter Management Module' interface. The left sidebar contains a navigation menu with 'Switch Tasks' expanded to 'Power/Restart'. The main content area is titled 'Switch Power/Restart' and contains the following table:

<input type="checkbox"/>	Bay	Type	MAC Address	IP Address	Pwr
<input type="checkbox"/>	1	Ethernet	00:05:5D:71:86:60	160.0.0.34	On
<input type="checkbox"/>	2		No switch present		
<input type="checkbox"/>	3		No switch present		
<input type="checkbox"/>	4		No switch present		

Below the table, there are three links: [Power On Switch Module\(s\)](#), [Power Off Switch Module\(s\)](#), and [Restart Switch Module\(s\)](#).

Select this choice to display the power status of the switch modules and perform the following actions:

- Turn on or turn off a switch module
- Reset a switch module

### Management

The screenshot shows the 'BladeCenter Management Module' interface. The left sidebar contains a navigation menu with 'Switch Tasks' expanded to 'Power/Restart' and 'Management' selected. The main content area is titled 'Switch Management' and contains the following links: [Switch Module 1](#), [Switch Module 2](#), [Switch Module 3](#), and [Switch Module 4](#).

Below these links is the 'Switch Module 1 (Ethernet)' configuration page. It shows the following configuration details:

**Current IP Configuration**  
 Configuration method: Static  
 IP address: 160.0.0.34  
 Subnet mask: 255.255.0.0  
 Gateway address: 0.0.0.0

**New Static IP Configuration**  
 Status: Enabled  
 To change the IP configuration for this switch module, fill in the following fields and click "Save". This will save and enable the new IP configuration.

IP address:   
 Subnet mask:   
 Gateway address:

At the bottom of the page, there is a link: [Advanced Switch Management](#).

Select this choice to view or change the IP configuration of the switch modules, ping the switch module, return a switch module to the default configuration, and start the configuration and management firmware that is in the switch module.

**Notes:**

1. Before you can access the switch module firmware, the following items must be set to **Enabled**:

- Switch module external ports
- External management for the external ports

From this page, click **Advanced Switch Management** → **Advanced Setup** and enable the items.

2. The initial user ID and password for the switch module firmware are:

- User ID: USERID (all capital letters)
- Password: PASSWORD (note the zero, not O, in PASSWORD)

See the *IBM @server BladeCenter Type 8677 User's Guide* for more information about basic configuration of the Ethernet switch module that is required for the BladeCenter unit.

See the documentation that comes with the switch module for details about the configuration and management firmware for the switch module. Documentation for the Ethernet switch module is on the *IBM BladeCenter Documentation CD*.

**MM Control**

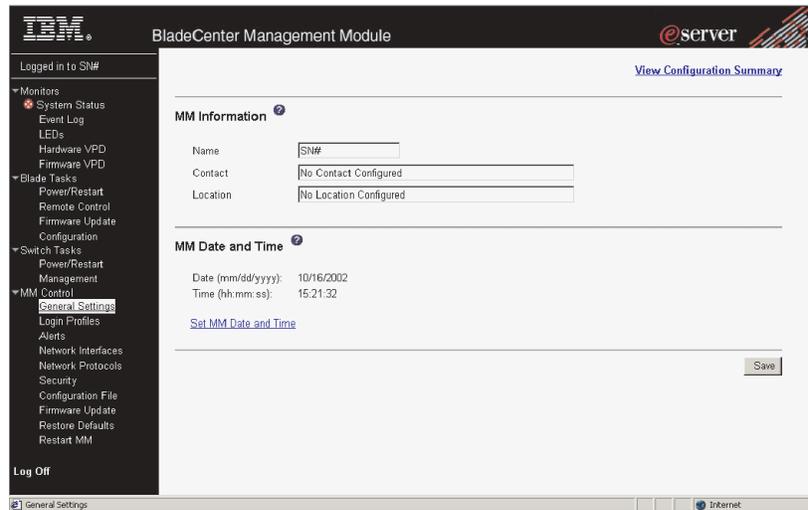
Select the choices in this section to view and change the settings or configuration on the management module whose Web interface you are logged into. This includes configuring the following items:

- The name of the management module
- Up to 12 login profiles for logging in to the management module
- How alerts are handled
- The management module Ethernet connections for remote console and for communicating with the switch modules
- Settings for the SNMP, SMTP, and DNS protocols
- Settings for secure socket layer (SSL) security

This also includes performing the following tasks:

- Backing up and restoring the management-module configuration
- Updating the management-module firmware
- Restoring the default configuration
- Restarting the management module

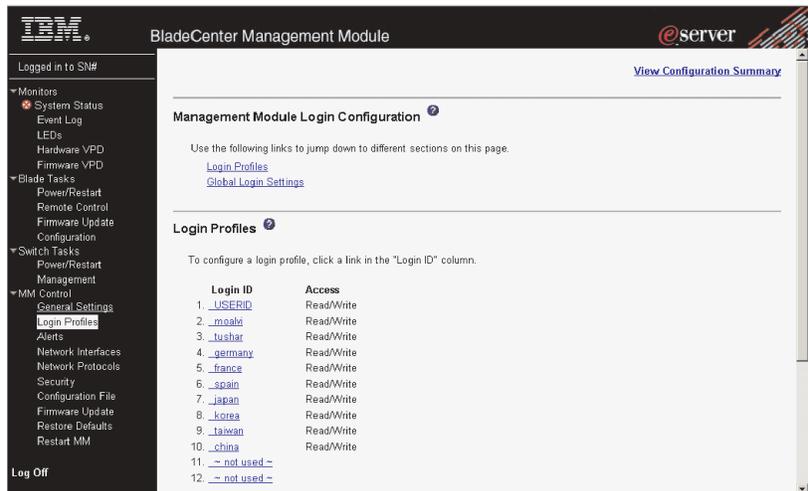
## General Settings



Select this choice to view or change the following settings:

- The name of the management module
- The name of the contact person responsible for the module
- The physical location of the management module
- The real-time clock settings in the management module

## Login Profiles



Select this choice to configure up to 12 login profiles for logging in to the management module, and to specify the lockout period after five unsuccessful login attempts. For each profile, specify the following values:

- Login ID
- Authority level (default is Read Only)
- Password (requires confirmation)

## Alerts

The screenshot shows the 'Management Module Alerts Configuration' page in the BladeCenter Management Module. The left sidebar contains a navigation menu with categories like Monitors, Blade Tasks, Switch Tasks, and MM Control. The main content area is titled 'Management Module Alerts Configuration' and includes links for 'Remote Alert Recipients', 'Global Remote Alert Settings', and 'Monitored Alerts'. Below these links is a section for 'Remote Alert Recipients' with a table listing 12 recipients, all currently set to 'not used'.

Name	Notification Method	Status
1. _mcahi	SNMP over LAN	Receives all alerts
2. _not used -		
3. _not used -		
4. _not used -		
5. _not used -		
6. _not used -		
7. _not used -		
8. _not used -		
9. _not used -		
10. _not used -		
11. _not used -		
12. _not used -		

Select this choice to specify which alerts (from lists of Critical, Warning, and System alerts) are monitored, which alert notifications are sent to whom, how alert notifications are sent (SNMP, e-mail, IBM Director), whether to include the event log with the notification, and other alert parameters.

## Network Interfaces

The screenshot shows the 'Management Module Network Interfaces' page. It features links for 'External Network Interface (eth0)', 'Internal Network Interface (eth1)', and 'TCP Log'. The 'External Network Interface (eth0)' section is expanded, showing configuration options for the interface, DHCP settings, and static IP configuration. The static IP configuration fields are filled with: IP address: 160.0.0.31, Subnet mask: 255.255.0.0, and Gateway address: 0.0.0.0.

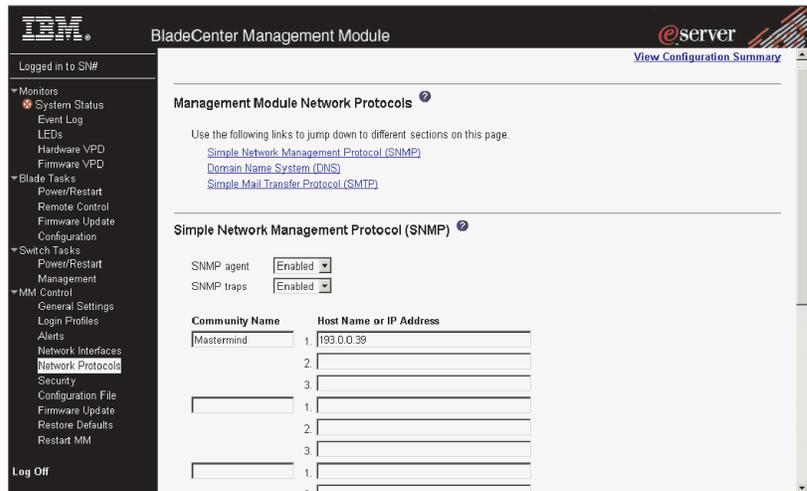
Select this choice to configure the two Ethernet interfaces: external (remote management and console), and internal (communication with the switch modules). You can also select this choice to view the TCP log.

**Note:** For switch communication with a remote management station, such as the IBM Director server, through the management module external Ethernet port, the switch module internal network interface and the management module internal and external interfaces must be on the same subnet.

- **External Network Interface (eth0)** - This is the interface for the remote management and console port.

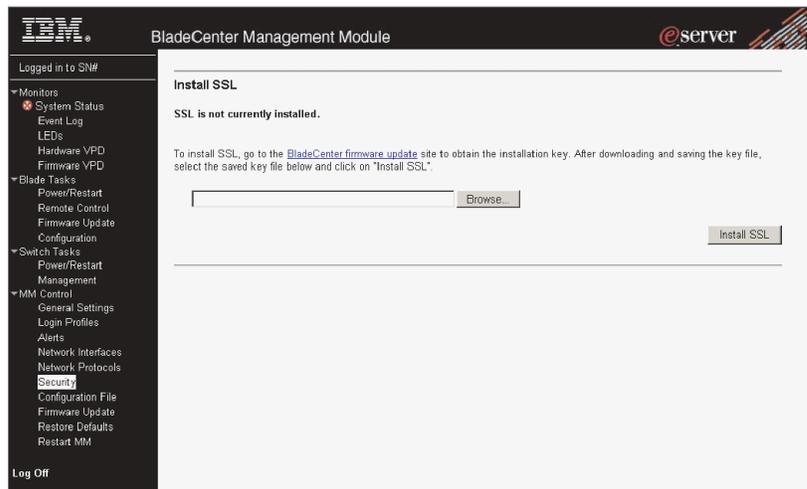
- **Interface** - Select **Enabled** (the default) to use the Ethernet connection.
- **DHCP** - Select one of the following choices:
  - **DHCP with rollover to static** (this is the default).
  - **DHCP only**
  - **Static only**
- **Hostname** - (Optional) This is the IP host name you want to use for the management module (maximum of 63 characters).
- **Static IP configuration** - You need to configure this information only if DHCP is disabled.
  - **IP address** - The IP address for the management module. The IP address must contain four integers from 0 to 255, separated by periods, with no spaces or consecutive periods. The default setting is 192.168.70.125.
  - **Subnet mask** - The subnet mask must contain four integers from 0 to 255, separated by periods, with no spaces. The default setting is 255.255.255.0
  - **Gateway address** - The IP address for your network gateway router. The gateway address must contain four integers from 0 to 255, separated by periods, with no spaces.
- **Internal Network Interface (eth1)** - This interface communicates with the switch module.
  - Specify the IP address to use for this interface. The subnet mask must be the same as the subnet mask in the external network interface (eth0).
  - View the data rate, duplex mode, maximum transmission unit (MTU), locally-administered MAC address, and burned-in MAC address for this interface. You can configure the locally-administered MAC address; the other fields are read-only.
- **TCP log** - Select this choice to view entries that are currently stored in the management module TCP log. This log contains error and warning messages generated by the TCP/IP code running on the management module, and might be used by your service representative for advanced troubleshooting. The log displays the most recent entries first.  
You can sort and filter entries in the event log.

## Network Protocols



Select this choice to view or change the settings for the SNMP, SMTP, and DNS protocols.

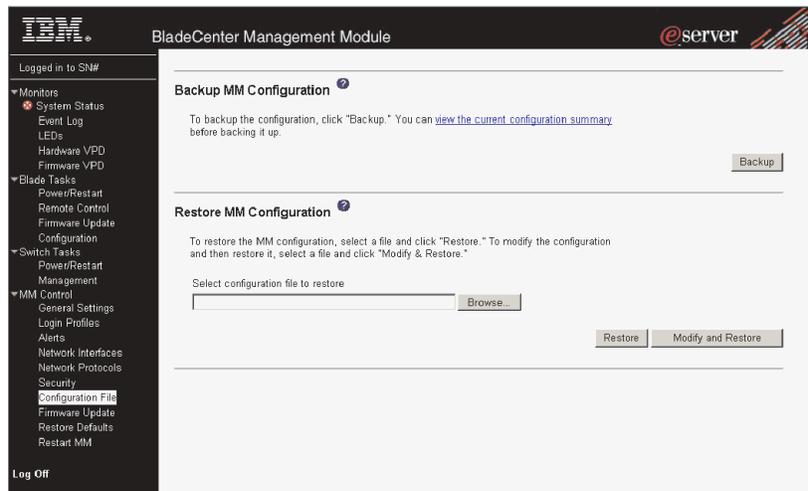
## Security



Select this choice to view or change the secure socket layer (SSL) settings. You can enable or disable (the default) SSL, and choose between self-signed certificates and certificates provided by a certificate authority (CA).

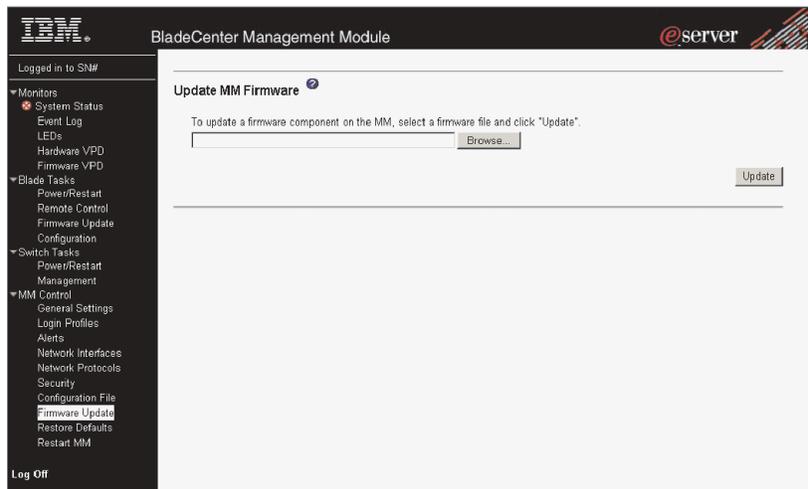
**Note:** The first time you select Security, you are directed to an IBM Web page for downloading the SSL installation key. After you load the key, the Security choice functions as described.

## Configuration File



Select this choice to back up or restore the management-module configuration file.

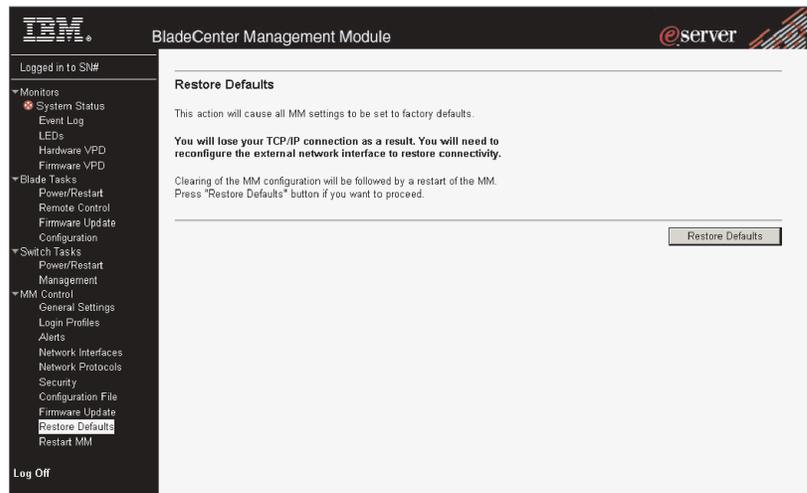
## Firmware Update



Select this choice to update the management-module firmware. Click the **Browse** button to locate the firmware file you want; then, click the **Update** button.

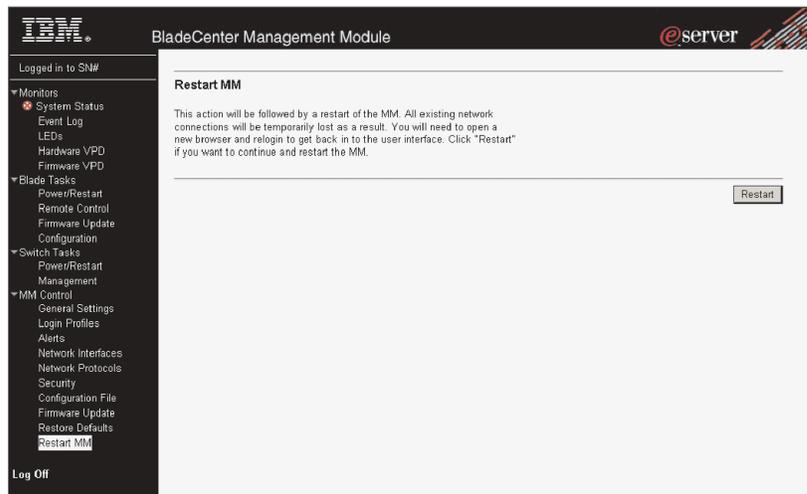
You can obtain the firmware files from the IBM Support Web site at <http://www.ibm.com/pc/support/>.

## Restore Defaults



Select this choice to restore the factory default configuration of the management module.

## Restart MM



Select this choice to restart (reset) the management module.

---

## Saving and restoring the configuration file

After you have configured the management module, you can save the configuration file to a diskette or other external media. Then, if the configuration in the management module becomes damaged or the management module is replaced, you can restore the saved configuration file to the management module. Use the management module Web interface to save and restore the configuration file (**MM Control** → **Configuration File**).

**Note:** If you cannot communicate with a replacement management module through the Web interface or the IBM Director programs, the IP address might be different from the IP address of the management module just removed. Press the IP reset button to set the management module to the factory default IP addresses; then, access the management module using the factory IP address (see “Configuring the management module for remote

access” on page 6 for the factory IP addresses) and configure the management module or load the saved configuration file.

---

## Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

*IBM Director of Licensing  
IBM Corporation  
North Castle Drive  
Armonk, NY 10504-1785  
U.S.A.*

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product, and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

---

## Edition notice

**© COPYRIGHT INTERNATIONAL BUSINESS MACHINES CORPORATION, 2002.  
All rights reserved.**

Note to U.S. Government Users Restricted Rights — Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

---

## Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

Active Memory	Predictive Failure Analysis
Active PCI	PS/2
Active PCI-X	ServeRAID
Alert on LAN	ServerGuide
BladeCenter	ServerProven
C2T Interconnect	TechConnect
Chipkill	Tivoli
EtherJet	Tivoli Enterprise
e-business logo	Update Connector
FlashCopy	Wake on LAN
IBM	XA-32
IntelliStation	XA-64
Light Path Diagnostics	X-Architecture
NetBAY	Xcel4
Netfinity	XpandOnDemand
NetView	xSeries
OS/2 WARP	

Lotus, Lotus Notes, SmartSuite, and Domino are trademarks of Lotus Development Corporation and/or IBM Corporation in the United States, other countries, or both.

ActionMedia, LANDesk, MMX, Pentium, and ProShare are trademarks of Intel Corporation in the United States, other countries, or both.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Linux is a registered trademark of Linus Torvalds.

Other company, product, or service names may be trademarks or service marks of others.

---

## Important notes

Processor speeds indicate the internal clock speed of the microprocessor; other factors also affect application performance.

CD-ROM drive speeds list the variable read rate. Actual speeds vary and are often less than the maximum possible.

When referring to processor storage, real and virtual storage, or channel volume, KB stands for approximately 1000 bytes, MB stands for approximately 1 000 000 bytes, and GB stands for approximately 1 000 000 000 bytes.

When referring to hard disk drive capacity or communications volume, MB stands for 1 000 000 bytes, and GB stands for 1 000 000 000 bytes. Total user-accessible capacity may vary depending on operating environments.

Maximum internal hard disk drive capacities assume the replacement of any standard hard disk drives and population of all hard disk drive bays with the largest currently supported drives available from IBM.

Maximum memory may require replacement of the standard memory with an optional memory module.

IBM makes no representation or warranties regarding non-IBM products and services that are ServerProven<sup>®</sup>, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. These products are offered and warranted solely by third parties.

IBM makes no representations or warranties with respect to non-IBM products. Support (if any) for the non-IBM products is provided by the third party, not IBM.

Some software may differ from its retail version (if available), and may not include user manuals or all program functionality.

---

## Electronic emission notices

### Federal Communications Commission (FCC) statement

**Note:** This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors or by using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

## Industry Canada Class A emission compliance statement

This Class A digital apparatus complies with Canadian ICES-003.

### Avis de conformité à la réglementation d'Industrie Canada

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

## Australia and New Zealand Class A statement

**Attention:** This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

## United Kingdom telecommunications safety requirement

### Notice to Customers

This apparatus is approved under approval number NS/G/1234/J/100003 for indirect connection to public telecommunication systems in the United Kingdom.

## European Union EMC Directive conformance statement

This product is in conformity with the protection requirements of EU Council Directive 89/336/EEC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a nonrecommended modification of the product, including the fitting of non-IBM option cards.

This product has been tested and found to comply with the limits for Class A Information Technology Equipment according to CISPR 22/European Standard EN 55022. The limits for Class A equipment were derived for commercial and industrial environments to provide reasonable protection against interference with licensed communication equipment.

**Attention:** This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

## Taiwanese Class A warning statement

警告使用者：  
這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

## Japanese Voluntary Control Council for Interference (VCCI) statement

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。



# Index

## C

- cabling
  - remote connection Ethernet port 5
- Class A electronic emission notice 27
- configuration file
  - restoring 23
  - saving 23
- Configuration/Setup Utility program 7
- configuring
  - BladeCenter unit 4
- connector
  - Ethernet
    - remote management and console 3
  - input/output 2
  - keyboard 3
  - PS/2 mouse 3
  - remote management 3
  - video 3

## D

- difficulty communicating with replacement module 23

## E

- electronic emission Class A notice 27
- error log
  - See event log
- Ethernet
  - configuring remote connection 6
  - port, cabling 5
- Ethernet activity LED 2, 6
- Ethernet connector, remote management and console 3
- Ethernet-link status LED 2, 5
- event log 10
- event log in alerts 19
- event log, viewing 10

## F

- FCC Class A notice 27

## I

- IP reset button 2, 23

## K

- keyboard connector 3

## L

- LEDs
  - active 2
  - error 2

## LEDs (continued)

- Ethernet activity 2, 6
- Ethernet-link status 2, 5
- power-on 2

## M

- mouse connector 3

## N

- network, connecting 5
- notes, important 26
- notices
  - electronic emission 27
  - FCC, Class A 27

## P

- port See connector 2
- power-on LED 2

## R

- remote console 14
- remote control 13
- remote management connector 3
- replacement module, difficulty communicating with 23
- restoring configuration file 23

## S

- saving configuration file 23

## T

- TCP log 20
- TCP log, viewing 20
- trademarks 26

## U

- United States electronic emission Class A notice 27
- United States FCC Class A notice 27
- utility, Configuration/Setup 7

## V

- video connector 3

## W

- Web browsers, supported 4







Part Number: 59P6535

Printed in U.S.A.

(1P) P/N: 59P6535

